

PRIVACERACLOUD 4.0: SECURE DATA SHARING FOR A DATA DRIVEN WORLD



Increased enterprise prioritization of data democratization, privacy, and security has led to an intense focus on the implementation of data control measures. Trying to strike the optimal balance among the three has proven to be a challenge, due to the lack of comprehensive understanding of policies, data, and systems by the various personas (policy drivers, policy implementers, and data consumers) involved in the enterprise data governance process. This results in siloed operations that constrain the analytics process, making sharing data internally and with business partners an inefficient process that can't keep up with the pace of business.

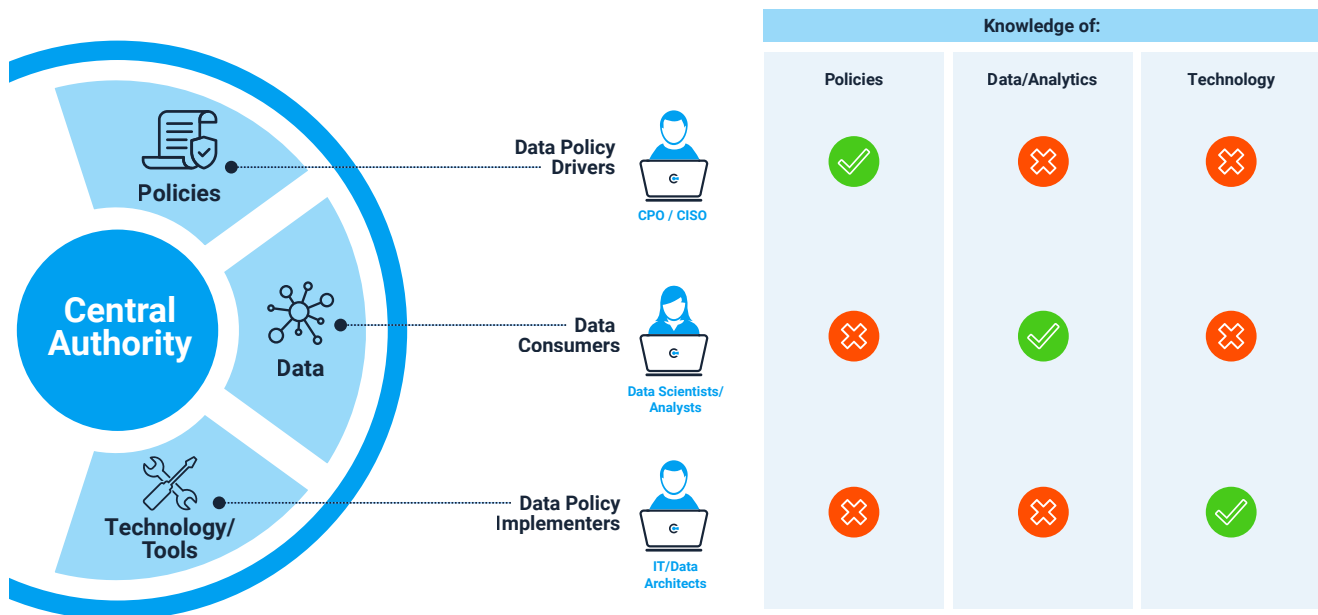


Exhibit1: Analytic personas do not have a comprehensive view of the data ecosystem

To drive latency out of the analytics process, PrivaceraCloud 4.0 introduces a new data sharing approach, **Governed Data Sharing**, that aligns the components of data access governance with the objectives of the personas involved in the analytics process. Governed Data Sharing deploys a distributed data governance model that delivers an unmatched level of efficiency to accelerate analytical initiatives by grouping functional data—such as sales, marketing, and finance—into **Data Domains**. This enables faster access to authorized data without compromising data compliance and privacy. For example, a Marketing Data Domain may consist of data sets related to customer/CRM, campaigns, website traffic, or third party demographics data stored in various cloud services.

Building Data Domains is Key to Sharing Data

The use of Data Domains alleviates the operational burden on IT by placing data owners in direct contact with data consumers to manage access requests, thereby greatly improving collaboration, flexibility, and responsiveness. After IT organizes functional data into Data Domains, access policies are automatically applied to data sets inside them. Although Data Domains are created by IT, they are owned by personnel with the most knowledge of that functional area. The “data owner” of a particular functional Data Domain are leaders in the relevant line of business, such as the VP of Sales, Marketing, or Finance. Data owners can create shared data sets within their Data Domains and make them discoverable by others in the company. PrivaceraCloud 4.0 provides each line of business the flexibility to control the distribution and consumption of their data, greatly improving data fluidity and utilization in the organization.

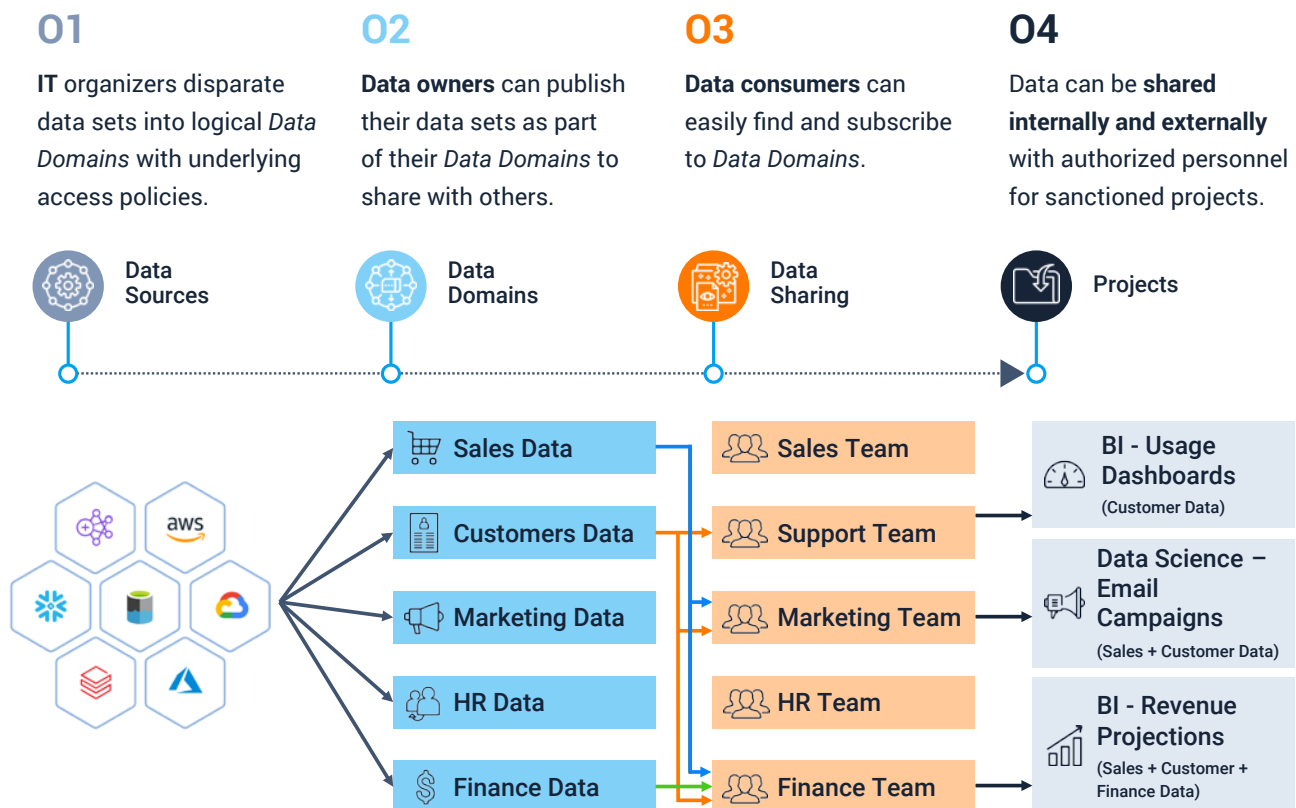


Exhibit 2: Framework for Governed Data Sharing

Data consumers, such as data scientists or business analysts, can browse through an inventory of data sets organized within a Data Domain. They can request access to the relevant data sets from the data owner by providing a reason for access. For example, in the diagram above, financial analysts can search and request relevant sales, customer, or finance data with the justification of needing it for a revenue projection project. Data Domain owners have the context and confidence that data will be used for authorized purposes by authorized personnel. Data scientists and analysts can be more productive, because they can subscribe to desired data sets within Data Domains, receiving automatic notifications, rather than repeatedly searching for data sets across on-premise and cloud services.



At the same time, IT no longer manages hundreds of access requests from data consumers. The task of requesting and granting access to data sets is now a simple interaction between data owners and data consumers, which can be accomplished with a click of a mouse. Because IT understands systems and knows about implementation details in this distributed framework, IT continues to maintain oversight of the data access governance platform to ensure visibility into all user activity, auditability of the access control policies, and proactively bring compliance violations to the attention of internal auditors.

KEY BENEFITS

Accelerate Business Agility

Data can be seamlessly shared internally and externally, as data can only be accessed by authorized personnel. With no rewriting of data access policies as they are automatically applied to Data Domains, secure data sharing becomes a 1-click operation between data owners/custodians and data consumers.

Maximize Data Visibility

Legal and security teams gain single-pane visibility into all user activities to proactively address any compliance violations. The IT team maintains the oversight of data across disparate cloud systems through a centralized console. The governance team, as well as the various data owners to the respective Data Domains, have instant visibility of data assets with out-of-box reporting, quick generation of custom reports, and alerts when sensitive data is accessed or moved.

Optimize Data & Team Collaboration

Central and local teams can build and collaborate on data access policies. Governed Data Sharing aligns the objectives and expertise of IT, data privacy and security officers, and data scientists, empowering them to operate as one team to optimize business efficiency and collaboration.

Ensure Authorized Data Access

Governed Data Sharing supports the distributed data access governance model, in which data stewards and custodians who are familiar with use cases in respective business domains grant end user access. The enforcement of policies is done closer to data and natively within applications, enabling superior performance, scalability, availability, and usability.

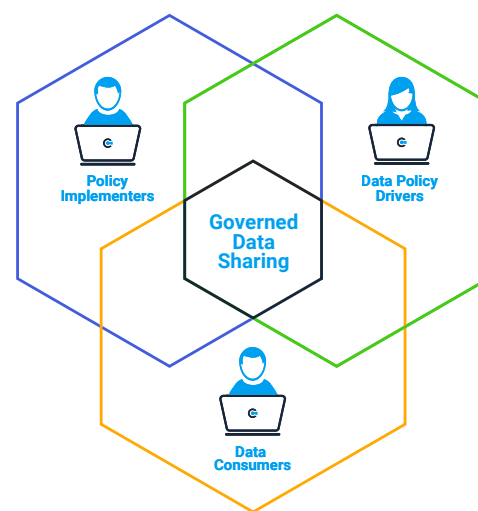


Exhibit 3: Governed Data Sharing aligns the objectives and expertise of the various personas involved in enterprise data governance

Ready to get started with Privacera?

Visit privacera.com to learn more,
or contact us at questions@privacera.com.